

COHN LIFLAND PEARLMAN
HERRMANN & KNOPF LLP
PETER S. PEARLMAN
Park 80 Plaza West-One
Saddle Brook, NJ 07663
Telephone: 201/845-9600
201/845-9423 (fax)

Liaison Counsel

COUGHLIN STOIA GELLER
RUDMAN & ROBBINS LLP
PAUL J. GELLER
DAVID J. GEORGE
JAMES L. DAVIDSON
BAILIE L. HEIKKINEN
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)

FARUQI & FARUQI, LLP
NADEEM FARUQI
EMILY C. KOMLOSSY
JAMIE R. MOGIL
369 Lexington Avenue, 10th Floor
New York, NY 10017-6531
Telephone: 212/983-9330
212/983-9331 (fax)

Co-Lead Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

In re HEARTLAND PAYMENT SYSTEMS, INC. SECURITIES LITIGATION) No. 3:09-cv-01043-AET-TJB
This Document Relates To:)
ALL ACTIONS.) CLASS ACTION
) AMENDED CONSOLIDATED
) CLASS ACTION COMPLAINT FOR
) VIOLATIONS OF THE FEDERAL
) SECURITIES LAWS
)

1. Co-Lead Plaintiffs Teamsters Local Union No. 727 Pension Fund, whose business address is 5940 West Montrose Avenue, Chicago, IL 60634, and Genesee County Employees' Retirement System, whose business address is 1101 Beach Street, Flint, MI 48502, (collectively, "Plaintiffs"), by and through their undersigned counsel, individually and on behalf of a proposed class (the "Class") of all purchasers of Heartland Payment Systems, Inc. ("Heartland" or the "Company") (NYSE: HPY) common stock between February 13, 2008 through and including February 23, 2009, inclusive (the "Class Period"), bring suit against Heartland, Robert O. Carr ("Carr") and Robert H.B. Baldwin ("Baldwin") (Heartland, Carr and Baldwin are sometimes collectively referred to as "Defendants").

2. Plaintiffs seek remedies under the Securities Exchange Act of 1934 (the "Exchange Act") as a result of the fraudulent scheme undertaken by Defendants and the economic loss suffered when the Company's true financial circumstances and future business prospects were revealed to the public through a series of partial disclosures that corrected market expectations for the Company. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act, 15 U.S.C. §§78j(b) and 78t(a), and Rule 10b-5 promulgated thereunder, 17 C.F.R. §240.10b-5.

INTRODUCTION AND NATURE OF THE ACTION

3. Heartland provides bank card payment processing services to merchants in the United States. The Company's services involve facilitating the exchange of information and funds between merchants and cardholders' financial institutions; and providing end-to-end electronic payment processing services to merchants, including merchant set-up and training, transaction authorization and electronic draft capture, clearing and settlement, merchant accounting, merchant assistance and support, and risk management.

4. On August 17, 2009, the U.S. Department of Justice handed down an Indictment against three individuals for perpetrating what is believed to be the largest data security breach in U.S. history (the "Indictment"). During the course of the conspiracy, the indicted co-conspirators hacked into Heartland's corporate computer network and stole approximately 130 million credit and debit card numbers and corresponding card data. As set forth in the Indictment, the security breach at Heartland occurred on December 26, 2007, and, as corroborated by Plaintiffs' investigation and detailed below, Defendants knew about the security breach as early as December 30, 2007.

5. Beginning on or about December 26, 2007, Heartland suffered a Structured Query Language ("SQL") Injection Attack on its corporate network that

resulted in malware being placed on its payment processing system.¹ The security breach at Heartland ultimately resulted in the theft of more than approximately 130 million credit and debit card numbers and corresponding card data, and is widely thought to be the largest data security breach in U.S. history.

6. The various confidential witness accounts detailed below, as corroborated by the details of the Indictment, evidence the fact that the **Defendants were made aware of the security breach as early as December 30, 2007.** Notwithstanding possession of this information, and not wanting to have to disclose that the Company's databases – which Defendants had touted as highly secure – were actually extremely vulnerable to attack, **for over a year** Defendants essentially denied that a security breach had occurred at Heartland. For instance, on February 13, 2008, less than two months after the breach had occurred, and in response to a barrage of questions regarding whether a recent increase in security spending was triggered by an incident at the Company such as a security breach, Carr falsely stated “[t]he incident was that

¹ SQL is a database computer language designed for managing data in relational database management systems. Its scope includes data query and update, schema creation and modification, and data access control. SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

new people came in and looked at our systems and found a number of things which were just not acceptable.” Baldwin followed up by falsely stating:

We did have one what I call minor incident in terms of our spam aspect of our firewalls so we did have one two-day period when our e-mails were overwhelmed with offers to do all kinds of different things. But there was no other incident and that by the way sort of burned out our firewall and we had to do some emergency preventative things on that. But it was nothing in terms of a data security external intrusion. It was re-evaluation. (emphasis added).

7. In the meantime, in addition to lying about the very existence of the breach, Defendants failed to contain the December 2007 security breach, failed to address the significant security vulnerabilities at the Company, and ultimately failed to prevent the theft of approximately 130 million credit card and debit card numbers from the Company’s databases. All the while, Defendants continued to publicly promote the safety of Heartland’s systems and the steps that the Company was taking to bolster security.

8. After more than a year of false statements, misrepresentations and omissions that Defendants hoped would alleviate the need to disclose the security breach and the subsequent negative impact on the Company, the sheer magnitude of the security breach forced Defendants’ hand. Specifically, in approximately October 2008, Visa contacted Heartland to report suspicious transactions stemming from accounts linked to Heartland’s systems. In response, Defendants for the first time – and a full ten months after the security breach occurred in December 2007 – hired

outside investigators to begin investigating whether Heartland had adequately contained the December 2007 security breach. It had not.

9. Thus, on January 20, 2009, Heartland publicly revealed for the first time what Defendants had been hiding for more than a year – that the Company’s payment processing system had been horrendously breached by malicious software, potentially exposing more than 130 million debit and credit card holders to identity theft and/or fraudulent activity. Heartland disclosed that intruders hacked into the computers it used to process 100 million payment card transactions per month for 175,000 merchants. As consumers used their credit and debit cards, so called “sniffer software” had been capturing their credit card and debit card information.

10. Upon this news, and the subsequent partial revelations through February 24, 2009 by Defendants concerning the scope of the breach, together with the uncertainty of the costs of the breach to the Company, shares of Heartland’s common stock declined \$21.84 per share, or approximately 80%, from its Class Period high of \$27.19 per share on September 19, 2008.

11. Notwithstanding their knowledge of the breach, throughout the Class Period, Defendants made false and misleading statements and/or omitted material information about the safety of Heartland’s computer network, never once revealing that a significant data breach had occurred. Defendants’ false and misleading statements cloaked the Company’s true financial condition and future business

prospects, and consequently caused the Company's common stock to trade at artificially inflated prices during the Class Period. When the truth was finally revealed through a series of partial disclosure events beginning on January 20, 2009, the Company's true financial condition and future business prospects were made known, the market's expectations were corrected, the artificial inflation came out of the price of Heartland's common stock, and Plaintiffs and the other members of the Class – purchasers of Heartland common stock during the Class Period – suffered tens of millions of dollars in damages.

12. In light of the foregoing, Plaintiffs bring this action seeking to recover the massive financial damages caused by Defendants' violations of federal securities laws.

JURISDICTION AND VENUE

13. This Court has jurisdiction over the subject matter of this action pursuant to §27 of the Exchange Act, 15 U.S.C. §78aa, and 28 U.S.C. §1331.

14. Venue is proper in the Judicial District pursuant to §27 of the Exchange Act, 15 U.S.C. §78aa, and 28 U.S.C. §1391(b). Many of the acts in furtherance of the alleged fraud and/or the effects of the fraud occurred within this District.

15. In connection with the acts, conduct, and other wrongs alleged in this Complaint, Defendants, directly or indirectly, used the means and instrumentalities of

interstate commerce, including but not limited to, the United States mails, interstate telephone communications, and the facilities of the national securities markets.

THE PARTIES

Plaintiffs

16. Teamsters Local Union No. 727 Pension Fund (“Teamsters”) was appointed Co-Lead Plaintiff on May 27, 2009. Teamsters purchased Heartland common stock during the Class Period at artificially inflated prices, and suffered damages when the truth regarding Heartland’s true financial condition and future business prospects was revealed. *See* Dkt. No. 5 at Exhibit “C.”

17. Genesee County Employees’ Retirement System (“Genesee County”) was appointed Co-Lead Plaintiff on May 27, 2009. Genesee County purchased Heartland common stock during the Class Period at artificially inflated prices, and suffered damages when the truth regarding Heartland’s true financial condition and future business prospects was revealed. *See* Dkt. No. 3 at Exhibit “2.”

Defendants

18. Heartland is a Delaware corporation that maintains its principal executive offices at 90 Nassau Street, Princeton, New Jersey 08542. Heartland provides bank card payment processing services to merchants in the United States. The Company’s services involve facilitating the exchange of information and funds between merchants and cardholders’ financial institutions; and providing end-to-end electronic payment

processing services to merchants, including merchant set-up and training, transaction authorization and electronic draft capture, clearing and settlement, merchant accounting, merchant assistance and support, and risk management. The Company also offers payroll processing services, including check printing, direct deposit, and accounting documentation, as well as related federal, state, and local tax deposits; gift and loyalty programs; electronic and paper check processing services; and micro payment and campus solutions, as well as sells and rents point-of-sale devices and supplies. Heartland is owned by the Company's shareholders, and the Company's common stock was listed and traded on the New York Stock Exchange during the Class Period.

19. Carr was, at all relevant times, the Chief Executive Officer ("CEO"), and Chairman of the Board of Directors of Heartland.

20. Baldwin was, at all relevant times, the President and Chief Financial Officer ("CFO") of Heartland.

21. Defendants Carr and Baldwin are sometimes hereinafter collectively referred to hereinafter as the "Individual Defendants."

22. Throughout the Class Period, Carr and Baldwin were responsible for ensuring the accuracy of Heartland's public filings and other public statements, and they both personally attested to and certified the accuracy of Heartland's public filings. During the Class Period – specifically on March 10, 2008, August 8, 2008 and

November 7, 2008 – Carr and Baldwin each signed certifications included in the Company's public filings stating:

- A. I have reviewed this quarterly report on Form 10-Q of Heartland Payment Systems, Inc.;
- B. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;
- C. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;
- D. The registrant's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act rules 13a-15(f) and 15d-15(f)) for the registrant and have:
 - 1. Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;
 - 2. Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

3. Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and
4. Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting.

E. The registrant's other certifying officer and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

1. All significant deficiencies and material weaknesses in the design operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record process, summarize and report financial information; and
2. Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

23. On those same dates, Carr and Baldwin each signed certifications included in the Company's public filings stating:

- A. The Report fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934; and
- B. The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

24. During the Class Period, each of the Individual Defendants, as senior executive officers and/or directors of Heartland, were privy to non-public information concerning the Company's business, finances, products, markets and present and future business prospects via access to internal corporate documents, conversations and connections with other corporate officers and employees, attendance at management and Board of Directors meetings and committees thereof and via reports and other information provided to them in connection therewith. Because of their possession of such information, the Individual Defendants knew or recklessly disregarded the fact that adverse facts specified herein had not been disclosed to, and were being concealed from, the investing public. Except to the extent set forth in this complaint as provided by confidential witnesses who are primarily former Heartland employees, Plaintiffs and other members of the Class had no access to such information, which was, and remains solely under the control of the Defendants.

25. Each of the Individual Defendants made knowingly false and misleading statements and/or omitted material information concerning, *inter alia*, the security breach that occurred at the Company in December 2007 and the extent of Heartland's vulnerability to security breaches, in the Company's earnings conference calls, during interviews with the media, and in other public presentations and speeches. These false and misleading statements were intended to and did artificially inflate the price of

Heartland's common stock, by misrepresenting Heartland's financial circumstances and future business prospects.

CLASS ACTION ALLEGATIONS

26. Plaintiffs bring this action as a class action pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased Heartland common stock during the Class Period. Excluded from the Class are Defendants, the officers and directors of the Company, members of their immediate families and their legal representatives, heirs, successors, or assigns, and any entity in which Defendants have or had a controlling interest.

27. Because Heartland has tens of millions of common shares outstanding, and because the Company's shares were actively traded on the NYSE, members of the Class are so numerous that joinder of all members is impracticable. According to Heartland's SEC filings, as of March 4, 2009, there were 37,442,292 shares of the Company's common stock outstanding. While the exact number of Class members can only be determined by appropriate discovery, Plaintiffs believe Class members number at least in the thousands and that they are geographically dispersed.

28. Plaintiffs' claims are typical of the claims of the members of the Class because Plaintiffs and all of the Class members sustained damages arising out of Defendants' wrongful conduct complained of herein.

29. Plaintiffs will fairly and adequately protect the interests of the Class members and have retained counsel experienced and competent in class actions and securities fraud litigation. Plaintiffs have no interests that are contrary to or in conflict with the members of the Class they seek to represent.

30. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy, since joinder of all members is impracticable. Furthermore, as the damages suffered by individual members of the Class may be relatively small, the expense and burden of individual litigation make it impossible for the members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

31. Questions of law and fact common to the members of the Class predominate over any questions that may affect only individual members, in that Defendants have acted on grounds generally applicable to the entire Class. Among the questions of law and fact common to the Class are:

- (a) Whether Defendants violated federal securities laws as alleged herein;
- (b) Whether Defendants' publicly disseminated press releases and statements during the Class Period omitted and/or misrepresented material facts;
- (c) Whether Defendants breached any duty to convey material facts or to correct material facts previously disseminated;

- (d) Whether Defendants participated in and pursued the fraudulent scheme or course of business complained of;
- (e) Whether Defendants acted willfully, with knowledge or severe recklessness, in omitting and/or misrepresenting material facts;
- (f) Whether the price of Heartland common stock was artificially inflated during the Class Period due to the material nondisclosures and/or misrepresentations complained of herein; and
- (g) Whether Plaintiffs and members of the Class sustained damages as a result of the decline in value of Heartland common stock when the truth was revealed and the artificial inflation came out and, if so, what is the appropriate measure of damages.

CONFIDENTIAL WITNESSES

32. Plaintiffs' allegations herein, concerning the falsity of Defendants' statements and the scienter of the Individual Defendants, are based, in part, on interviews with dozens of former Heartland employees and others with knowledge of the facts underlying Defendants' fraud. Each of the confidential witnesses ("Confidential Witnesses") who provided Plaintiffs' counsel with the information alleged herein held a position with Heartland that permitted her or him direct access to the information provided by each.

33. One former Heartland employee was an independent contractor who worked as a Senior Software Developer at Heartland from approximately mid-2006 through February 2008. The former Senior Software Developer worked on a system for credit card processing at Heartland called “Passport.” Another former Heartland employee worked as a Business Analyst in the Company’s Frisco, Texas office from October 2006 until August 2008. Another Heartland former employee was a Senior Developer from mid-2007 until the Spring of 2008. This former employee had information concerning the timing of the security breach and knowledge of the breach within the Company.

34. Another former Heartland employee worked for Heartland from January 2005 until May 2008, attaining the title of Director of Application Development. This former employee had knowledge of the systems used by Heartland to process credit card payments and the destabilizing employee turnover at the Company. Another former Heartland employee worked as a Senior Programmer in the Frisco, Texas office from approximately April 2007 through May 2008. The former Senior Programmer was hired to build monitoring and other security processes into Passport.

35. As demonstrated below, the information provided by the Confidential Witnesses corroborated not only each other’s accounts of Defendants’ fraud, but also post-Class Period events concerning the details of Defendants’ fraud, culminating in the indictment of the alleged criminals behind the security breach.

SUBSTANTIVE ALLEGATIONS

Background

36. Heartland was founded in 1997 and, together with its subsidiaries, provides bank card payment processing services to more than 250,000 merchants and businesses in the United States and Canada. The Company's services involve facilitating the exchange of information and funds between merchants and cardholders financial institutions; and providing end-to-end electronic payment processing services to merchants, including merchant set-up and training, transaction authorization and electronic draft capture, clearing and settlement, merchant accounting, merchant assistance and support, and risk management. Heartland provides additional services to its merchants including payroll processing, gift and loyalty programs, paper check processing, and sells and rents point-of-sale devices and supplies.

37. According to the former Director of Application Development, there were two main computer systems Heartland used for processing credit card transactions. "Exchange" was the system that took credit card information transmitted from merchants and sent it on to the credit card associations, such as Visa or Mastercard, for authorization. "Passport" was the "settlement claiming system," which paid the merchant and deducted the interchange amounts charged in connection with the transaction by Visa or Mastercard. According to the former Senior

Programmer, Passport was also called “the Pipeline.” The former Senior Programmer said that Passport was not just one process – it was made up of numerous smaller programs that batch through twelve systems. According to the former Senior Programmer, Passport “is manual, with cycles, transaction clearing and ACH funding all set as different manual steps.”

38. To illustrate how the Passport and Exchange systems work, the former Director of Application Development described the following hypothetical transaction: For a \$100 purchase at a store, the merchant transmits the credit card information to Heartland, and Heartland uses its Exchange system to send the information on to the credit card company. The credit card company then communicates back to Heartland that the transaction is authorized, and Heartland communicates that back to the merchant. Heartland then calculates the interchange charge and reduces the payment by \$1.50 in interchange fees charged by Visa or Mastercard. Heartland also then reduces the payment further for the fees Heartland charges to merchants.

39. The former Business Analyst corroborated the statements made by the former Director of Application Development that the credit card processing that Heartland performs for merchants depends on two processes, with Exchange being the credit card authorization system and Passport being the system that processes and transmits payments to merchants. According to the former Senior Business Analyst,

the Exchange system accepts credit card information and point of sales transaction amount information from merchants and then passes the information on to the credit card associations. The associations then confirm that the credit card is legitimate and working and that the transaction is authorized by the card issuer.

In 2007, the Company’s “Passport” and “Exchange” Systems Were Suffering From Pervasive Security Vulnerabilities

40. The former Business Analyst was responsible for managing bi-annual system enhancements that were required by the card associations, which were primarily Visa and MasterCard. While Heartland also worked with the American Express and Discover card associations, the former Business Analyst’s work focused primarily on Visa and Mastercard. The enhancements the former Business Analyst oversaw and helped implement involved changes in how data was transmitted to the card associations.

41. For example, when the card associations launched new types of cards, such as the World card, there were new data elements associated with those cards that had to be communicated from Heartland to the card associations. According to the former Business Analyst, there were also various technical enhancements required by the card associations that she/he helped implement at Heartland.

42. According to the former Senior Software Developer, Heartland “got in over their head” with the Passport software based on how it was originally developed and the failure to perform a significant overhaul or re-engineering over the years.

Initially, Heartland did not have its own settlement software and so the Company licensed Vital for the “back end” essential settlement functions. According to the former Senior Software Developer, Heartland “developed Passport to replace Vital.” Once Passport was barely operational, Heartland wanted to start pulling every merchant off Vital and onto Passport as soon as possible. According to the former Senior Software Developer, Heartland began moving thirty merchants off Vital on to Passport every day for a month. Then every month after that the number of merchants moved to Passport from Vital doubled, until Heartland was relying only on Passport and was no longer using Vital at all.

43. According to the former Senior Software Developer, all of the migrations were done by hand. The former Senior Software Developer was brought in to develop an automated way to manage changes to how merchants are processed. The Passport initial development was rushed “and put into production very quickly” so Heartland could save money by relying less on the licensed Vital software.

44. According to the former Senior Software Developer, the initial Passport development was built to meet the minimum business needs of then existing types and number of merchants and nothing more. It was “like building a house with only half a foundation and not letting the concrete dry before you start building. ***There was no security, compliance, reporting or banking support.*** There were lots of little problems. It was like a stripped down plane with limited functions, but it could still

technically fly, as long as you didn't add too many passengers or encounter any new problems. It was just enough to get rid of Vital."

45. Unfortunately, according to the former Senior Software Developer, Heartland added more and more functions and merchants and significantly expanded the number of transactions processed. The result, according to the former Senior Software Developer, was a slow and overburdened software system with significant security vulnerabilities. "A lot of times we would almost miss the Federal [deadline] window to process transactions [so that merchants could be paid] because Passport was running so slowly." According to the former Senior Software Developer, the slow processing was a symptom of larger problems that stemmed from the haphazard, early development of Passport and the failure to implement automated processes such as security, compliance, reporting and banking processes.

46. *The former Senior Software Developer said that she/he always expected to hear that Heartland lost their Visa certification to process Visa card transactions because Heartland security was so lax and vulnerable.* According to the former Senior Software Developer, there were vulnerabilities in "**Passport that could have been exploited by any employee with access to the Passport database, which is pretty much everyone [in the Frisco office] . . . There were very serious vulnerabilities in Passport.**"

47. For instance, according to the former Senior Software Developer, a greedy or disgruntled programmer would only need to log in to a Passport production server with a production password. The production password “was known by every person on the Passport team, and the passwords hadn’t changed for years” as of the time the former Senior Software Developer left the Company in February 2008. The passwords “hadn’t changed from the day I got there.”

48. According to the former Senior Software Developer, Heartland utilized eight application servers and one huge database server. All customer service employees in the Jeffersonville, Indiana office who take complaints or support calls from merchants checked internal Heartland webpages that explain how to answer various questions. The former Senior Software Developer stated that “[a]ll those webpages hit the same database server [Heartland was] using to process transactions. There was only one copy of the database. Queries from support developers or others would make production run slow.” According to the former Senior Software Developer, anytime a support developer had to look up information for a customer service representative or to develop a new webpage to answer a question, the process required accessing the central database server.

49. According to the former Senior Software Developer, Heartland customer service employees had database passwords and could do queries directly into the database if they wanted to. The customer service employees could not change

anything, but they could read it. According to the former Senior Software Developer, the information the customer service employees had access to included “a database table that included extensive information about Heartland’s merchant customers, including merchant name, date of birth, and social security numbers. The merchant table is completely unencrypted.” This was corroborated by the former Senior Programmer, who noted that critical merchant information, including social security numbers, were not encrypted in Passport. According to the former Senior Programmer, this purportedly confidential information was just stored in “plain text” in the database. The former Senior Software Developer, the former Senior Programmer and other developers raised this problem to the Chief Technology Officer (“CTO”) and others, but no one responded to their concerns, despite the fact that the security of Heartland’s systems were absolutely critical to Heartland’s core business. Because of this relationship to Heartland’s core business, there is a reasonable inference that can be drawn that Carr or Baldwin knew or recklessly disregarded the vulnerabilities that were ultimately exploited, resulting in the December 2007 security breach that put 130 million consumers’ credit cards and debit cards at risk.

50. According to the former Senior Software Developer, if a Heartland employee wanted to steal money, she/he could just open a bank account for herself/himself at one of the banks that Heartland worked with. Then the Heartland employee could just direct that Heartland send money into her/his own account.

According to the former Senior Software Developer, Heartland did not use any fraud software to prevent this sort of internal fraud.

51. This was corroborated by the former Senior Programmer, who stated that it would have been easy to create a false merchant account to embezzle large sums from the Company. According to the former Senior Programmer, a false merchant account could be created “no matter where you are in the Company. You could create false transactions. You can edit the database with small transactions fed into the database to rip off the system. The margin of error was several hundred thousand dollars. We were constantly putting out multi-million dollar fires [because of huge mistakes in the transaction processes.]”

52. According to the former Senior Programmer, all the developers in the Frisco office had user names and passwords for every database and file. According to the former Senior Programmer, there were no tools for auditing transactions to determine where they originated or who input them. A Heartland employee who created a false merchant account and input false batch sales transactions into the database for that merchant to be paid by Heartland would not even need to use another employee’s passwords to evade detection. According to the former Senior Programmer, there were no tools for Heartland to know that the transactions originated internally nor who originated them. The former Senior Programmer stated “[n]o record is kept. Things just happen.”

53. The former Business Analyst explained that the overall approach to security at Heartland was very lax. According to the former Senior Business Analyst, that was true of physical security as well as electronic security. The former Senior Business Analyst stated that “[t]he floors were wide open. Anyone could walk on the floors. There was not much security.” Considering how many credit card numbers Heartland handled and how much confidential information Heartland retained about its merchant customers, the former Business Analyst “would have expected more physical security, file security, policies for non-employees [limiting their access].” According to the former Business Analyst, there was “not really any laptop security. Many employees were issued laptops to do work from home and they used a VPN [virtual private network] to port into the Heartland intranet. But there were no restrictions on website access internally or on laptops.”

54. According to the former Business Analyst, there were four entrances into the Heartland building in Frisco, Texas and only one of those was manned by a reception desk. According to the former Business Analyst, it was not uncommon for people wearing maintenance clothes to roam round within the Heartland office, unbadged and unescorted. “No one would be watching them.” The former Business Analyst knows that other Heartland employees “notified people about the security problems and were ignored.”

55. The former Senior Software Developer confirmed statements from the former Business Analyst that it was possible to gain access to the Frisco office by following behind employees and coming in one of four entrances behind them. Though the actual Passport servers are in secure bunkers, according to the former Senior Software Developer, a would-be thief would not need physical access to a server to capture information or load malware. If someone snuck into the Frisco office, which was possible, they could conceivably have loaded a key logger onto one of the computers used by high level employees to steal passwords or other information. According to the former Senior Software Developer, a thief could then use that information to learn whatever they needed to install the malware that Heartland has since said was the method used in the breach it publicly disclosed in January 2009.

56. The former Senior Software Developer eventually resigned out of frustration because she/he realized the problems in Passport were eventually going to damage the Company. According to the former Senior Software Developer, if Passport crashed, was infiltrated or damaged, Heartland would effectively be out of business because it would be unable to process transactions.

57. The former Business Analyst said that Carr's public statements in which he portrays himself and Heartland as being long-standing advocates for more encryption and better data security are not accurate. "*The discussions about*

encryption are so not them.” Data security was “nothing they ever cared about. To claim now they always cared about it is very hypocritical from how they acted in the past. It is very, very contradictory to how they always acted.”

Beginning in Late 2007, Heartland Experiences Rapid and Destabilizing Employee Turnover

58. According to the former Director of Application Development, in mid-2007, the then-CTO – Brooks Terrell (“Terrell”) – left the Company. Defendants then made a programmer – Alan Sims (“Sims”) – the new CTO. According to the former Senior Software Developer, prior to becoming CTO in late 2007, Sims was just a “regular little software developer on the Exchange team.” With his promotion, Sims went straight from software developer to CTO, which, according to the former Senior Software Developer, jumped approximately six levels of corporate hierarchy. Typically, the hierarchy of titles was Software Developer who reported to a Senior Software Developer, then Architect, then Director, then Senior Director.

59. According to the former Senior Software Developer, Sims had no qualifications to support the major jump to CTO. Sims did not have significant management experience and was not a particularly accomplished programmer. According to the former Senior Software Developer, many individuals left Heartland following Sims’ promotion. Sims took over and it became “promotion bingo” for his friends from the Exchange team. Many people who had worked for the prior CTO or who just stood in the way of promotions for Sims’ cronies were let go in short order in

late 2007 through mid-2008. According to the former Senior Software Developer, instead of a team focused on developing good software, “it became one political nightmare.”

60. According to the former Director of Application Development, the new CTO “pretty much chucked out the old guard who had reported to the old CTO.” The former Business Analyst also confirmed that after Sims took over as CTO, Sims systematically fired skilled Heartland IT employees in the Frisco office who had been hired by Terrell. The former Director of Application Development said that in addition to removing those employees, Sims engaged in “a political play” and promoted his friends to the newly vacant important positions. “A lot of his friends were suddenly promoted.”

61. According to the former Business Analyst, it was shocking both because of the “limited experience” of those newly promoted and because of the speed with which the old experts were removed and replaced. The processes at Heartland were crucial to the success and stability of the Heartland business and it seemed imprudent to change so many crucial employees so quickly. The former Business Analyst thought of this transition as “the return of the underdogs.”

62. According to the former Senior Software Developer, the rapid terminations that followed Sims’ promotion included Steve Reynolds, who had been

the number two Heartland technology professional beneath the former CTO. Sims also presided over the firing of IT managers at Heartland.

63. Thereafter, according to the former Senior Software Developer, Mark Wilson (“Wilson”) was promoted to Director of Passport Development. According to the former Senior Software Developer, Wilson initially worked on the Exchange team and was then moved to leadership of Passport in late 2007 or early 2008. According to the Former Senior Software Developer, Wilson’s promotion was based on his personal friendship with Sims. According to the former Senior Software Developer, Wilson was a bad programmer and manager who resisted all efforts to improve Passport and make it more secure.

64. For instance, the former Senior Software Developer tried to work with Wilson to address the limitations of Passport, including that it was not robust or scaleable to support a growing number of transactions. Wilson did not want to hear anything the former Senior Software Developer or anyone else had to say about limitations in Passport or resulting vulnerabilities caused by those limitations.

65. The former Senior Programmer relayed to Wilson a problem he found with Passport involving batches of transactions disappearing from the system. According to the former Senior Programmer, Wilson believed Passport “was his baby” and resisted any criticisms or suggestions about how to improve it.

66. For six months, the former Senior Programmer, the former Senior Software Developer and others worked on automating Passport. They had meetings with the other developers ever day, including Rod Stallings (“Stallings”), who was, at that time, in charge of Operations.² According to the former Senior Programmer, Wilson, as the head of Passport, logically would have attended the meetings, but he never attended. According to the former Senior Programmer, Wilson was upset someone else was pointing out quality issues with his code.

67. According to the former Senior Software Developer, Heartland put itself at serious risk by firing a large number of its most qualified programmers and experts within a short period of time. According to the former Senior Software Developer, Sims compounded those risks by promoting inexperienced and unqualified employees to replace the experts. The chief qualification of the newly promoted appeared to be their loyalty and or friendship with Sims. According to the former Senior

² Before the former CTO Terrell had resigned, he had hired Stallings who previously worked at Southwest Airlines. According to the former Senior Software Developer, “[s]tallings was a great guy. Terrell created a new division at Heartland called Operations and put Stallings in charge.” According to the former Senior Software Developer, Wilson had a disagreement with Stallings. After the disagreement, Sims fired Stallings. According to the former Senior Software Developer, “[p]retty much anyone who stayed [at Heartland] was either scared or too comfortable with their paycheck [to take a stand and leave]. Things quickly went downhill from there.”

Programmer, “[s]ome of the dumbest people I have ever met were being promoted,” primarily because they were seen as loyal to Sims or Wilson.

68. After the Company finally publicly disclosed the breach in January 2009, the former Senior Software Developer sent Carr an email basically saying “I told you so.” The reason the former Senior Software Developer ultimately told Carr “I told you so,” was because it was well known that internal security at Heartland was woefully inadequate for the Passport system. In her/his email, the former Senior Software Developer attributed weaknesses and security vulnerabilities in Passport to Wilson’s management. Carr wrote back and notified the former Senior Software Developer that Wilson was no longer in charge of Passport development. Of course, given the fact that Heartland’s computer systems were already compromised, this was too little, way too late.

A Major Security Breach Occurs at Heartland in December 2007 – Defendants Try to Sweep It Under the Rug

69. While employed at Heartland, the former Senior Developer conducted code-review to check the other developers’ work before new web based applications or revisions were implemented. The former Senior Developer also helped determine which developers were assigned to which projects and she/he attended meetings that determined how the IT department was allocating resources.

70. Additionally, the former Senior Developer was in charge of a web-based application called Payroll Manager. According to the former Senior Developer, the

Payroll Manager application provided payroll functions for outside entities that contracted with Heartland for payroll service. According to the former Senior Developer, Heartland acquired the Payroll Manager application when it purchased another company that was based in the Cleveland, Ohio area. Though Heartland employees who primarily used the Payroll Manager application were based in the Company's Ohio office, the former Senior Developer was responsible for maintaining the application out of the Company's Jeffersonville, Indiana office.

71. According to the former Senior Developer, Payroll Manager is written in Active Server Pages (“ASP”), which is vulnerable to breaches by hackers.³ ASP is much less secure than the modern ASP.NET. According to the former Senior Developer, approximately 70 to 80% of Heartland applications were written in classic ASP, which was “not that secure compared to ASP.NET.”

72. The former Senior Developer took a planned vacation beginning on December 22, 2007, with the intention of returning to the office on January 2, 2008. On December 30, 2007, the former Senior Developer received a voicemail from another Senior Developer – Alex Shull (“Shull”). The timing of this voicemail was

³ ASP, also known as Classic ASP or ASP Classic, was Microsoft’s first server-side script engine for dynamically-generated web pages. It has now been superseded by ASP.NET.

unusual given that it was a Sunday and the former Senior Developer did not socialize with Shull outside of work or speak with him on weekends.

73. When the former Senior Developer returned the telephone call, Shull told her/him that Shull was calling because he did not want the former Senior Developer to be blindsided when she/he returned to work. Shull informed the former Senior Developer that Heartland had suffered a breach in the Payroll Management application. ***Shull told the former Senior Developer that the breach was an SQL Injection Attack.***

74. When the former Senior Developer arrived at the office on January 2, 2008, after the holidays, she/he learned more about the breach. The breach was a sophisticated attack. According to the former Senior Developer, the Payroll Manager application had essentially two fields for inputting username and password so people using the application could log in to it. ***According to the former Senior Developer, the hackers were able to input strings of code into those fields that migrated into the Company's server and then executed a new program injected by the hackers.***

75. Shull told the former Senior Developer that Heartland discovered the breach because the Company's database in Texas was running extremely slow. According to the former Senior Developer, the fact that the database was running slowly indicated that the hackers were able to do something within the Heartland server. According to the former Senior Developer, if the hackers had just injected

harmless code, it is unlikely that it would have noticeably slowed the database. The former Senior Developer believed the hackers were transmitting data out from the database or server because otherwise the hack would not have slowed the database down so noticeably. *According to the former Senior Developer, in an attempt to prevent the transmission of data outward by the hackers, Heartland had to block the server from transmitting data to IP addresses in the Netherlands.*⁴

76. When the former Senior Developer returned to the office on January 2, 2008, she/he and Shull were putting out fires for the entire month of January related to the breach. According to the former Senior Developer, “[a] lot happened in January. It was very stressful.” According to the former Senior Developer, the Payroll Manager application was also used to generate payroll for Heartland employees. According to the former Senior Developer, the payroll data included the social security numbers, addresses and other highly confidential personal information of Heartland employees and the employees of other companies who used the Heartland Payroll service. This data was not encrypted in the Heartland database. Thus, according to the former Senior Developer, the breach through Payroll Manager

⁴ According to the Indictment against the co-conspirators who perpetrated the security breach, the indicted co-conspirators used internet-connected computers in the ***Netherlands***, the Ukraine, Latvia, Illinois, California and New Jersey to stage the security attacks and transmit data from the Heartland computer systems.

exposed all the Heartland employees and other payroll service users to identity theft because the hackers could easily get names, social security numbers and addresses.

77. According to the former Senior Developer, there were numerous links between Heartland servers and databases so applications could pull data from different databases automatically. Because of the interconnections, the former Senior Developer believed it is possible that the hackers who breached Heartland in late 2007 were able to insert the code that led to the credit card and debit card thefts the Company claims began in May 2008. According to the former Senior Developer, hackers could use their successful breach in 2007 (which Defendants never disclosed during the Class Period) to have code migrate from where the hackers breached the payroll application into other parts of the Heartland network or applications.

78. The former Senior Developer attended a meeting with Shull and all the developers in Jeffersonville to discuss the attack, though Jeff Compton (“Compton”) – the Executive Director of IT – did not attend. According to the former Senior Developer, Compton was aware of the attack because Compton told the former Senior Developer that the Payroll Manager and other applications were visible to Google and other search engines, which made them more vulnerable to being found and exploited by hackers. Compton tasked the former Senior Developer with making those applications invisible to Google and other major search engines and getting them removed from search engine search results. According to the former Senior

Developer, that way only Heartland customers or employees who needed to use the pages would know the page addresses and how to get to them.

79. Following the undisclosed security breach, though Heartland seemed focused on educating its developers about SQL Injection Attacks and figuring out a way to make those attacks less likely in the future, according to the former Senior Developer, there was no discussion of what Heartland was doing to address the breach that had already occurred. According to the former Senior Developer, if Heartland wanted to protect itself after the Payroll Manager breach, the Company should have built a new server with a clean copy of the operating system. Then the Company should have installed a clean copy of the database application on that new server, and then migrated the data over to the new server. According to the former Senior Developer, this would ensure that the server and database did not have any malicious code hidden on it.

80. However, according to the former Senior Developer, this was never done by Heartland at least through the date when the former Senior Developer left the Company. The former Senior Developer believes *“they didn’t successfully annihilate the 2007 breach problem. They should have started over to make sure it was gone.”* Though the former Senior Developer was never contacted or worked with any professional contractors brought in to assess the breach, its effects or how to remediate it, according to the former Senior Developer, all the post-2007 breach work

appeared to be handled in-house and was focused solely on reducing future vulnerability, not addressing the breach that had already occurred.

81. Sims – Heartland’s CTO – came to the Jeffersonville office in January 2008 and briefly discussed the breach with the former Senior Developer. Sims was “aware of the problem.” The former Senior Developer believes Sims certainly would have alerted Carr and Baldwin about the breach, as the protection of consumers’ private, personal information was at the very core of Heartland’s business. According to the former Senior Developer, the following individuals, all of whom are still employed at Heartland, also definitively knew about the breach: (1) Senior Developer Shull; (2) Executive Director of IT Compton; (3) Mindy Moretti – Senior Business Analyst; (4) Kent Cissell – Project Manager; (5) Steve Shumate – Senior Developer; and (6) Nicholas McRae – Junior Developer.

82. George Duke (“Duke”) was a Senior Developer/Build Manager at Heartland. According to the former Senior Developer, there were a number of Heartland developers. To coordinate all their work, Duke’s job was to make sure that the individual parts each developer was coding would integrate correctly into a larger application. The former Senior Developer wrote to Duke after the breach was announced in January 2009 and Duke responded that “***he was not surprised.***” The former Business Analyst stated that she/he was also “***not at all surprised by the breach***” because “***security was not there.***” Additionally, the former Senior

Programmer was not surprised about the breach and stated “[w]e thought a breach was likely.”

83. **The former Senior Developer could not understand why there was never any public disclosure [prior to January 2009] by the Company of the Payroll Manager breach or communication with Heartland employees to let them know they were vulnerable to identity fraud because of the breach.**

84. After the breach was finally announced in January 2009, Heartland claimed that it had long been conducting “penetration testing” to look for vulnerabilities or malicious code. According to the former Senior Developer, penetration testing was not being conducted prior to March 2008, notwithstanding Defendants’ knowledge of the breach in December 2007. According to the former Senior Developer, she/he does penetration testing at her/his current job and those tests “always turn up something.” Often the penetrations are ineffective or do not actually do anything, but the tests always raise issues for follow-up.

Defendants Fail to Correct the Pervasive Security Vulnerabilities at the Company

85. According to the former Business Analyst, Brian Ruberts (“Ruberts”) was the head of the Heartland network and the person ultimately responsible for Heartland compliance with the Payment Card Industry Data Security Standards

(“PCI”) rules.⁵ The former Business Analyst had experience working with PCI from her/his prior employment. According to the former Business Analyst, every year Heartland had to get re-certified as PCI compliant.

86. In 2008, Heartland was late in satisfying its PCI re-certification. The former Senior Business Analyst brought this to Ruberts’ attention and asked to schedule a meeting with him to discuss what needed to be done to be re-certified. The former Business Analyst then met with Ruberts in his office that was by the front reception desk in the Frisco office for approximately 20 minutes. According to the former Business Analyst, during the meeting, it became clear that **“Ruberts did not know what PCI was.”**

87. During their meeting, the former Business Analyst explained that Ruberts should schedule a meeting with every department head and provide them with self-assessment forms so that the individual department heads could identify any areas that needed to be remediated or brought up to standards. According to the former Business Analyst, those self-assessments should have included developers for Passport and Exchange because any vulnerabilities in either system impacted PCI compliance. Ruberts thanked the former Senior Business Analyst for her/his input,

⁵ PCI is a standard from the PCI Security Standards Council, developed to ensure financial data security standards.

but then did not follow any of her/his recommendations. According to the former Business Analyst, there were no meetings with department heads or other efforts to take PCI compliance seriously.

88. According to the former Business Analyst, the extent of PCI compliance education provided by Ruberts and Heartland to the various employees in the Frisco office was a single 8 ½ by 11 piece of paper posted near the copier that had a small number of very basic bullet point rules on it. For example, “don’t send credit card numbers in emails.’ [This security effort was] inconsequential and easy to miss. But there were no legitimate education efforts or security efforts.”

89. According to the former Business Analyst, to get PCI compliance approval requires an independent authorized security company to assess compliance. But a compliance assessment “is just a snapshot of one moment in time.” According to the former Business Analyst, the independent assessment entity is known as a Quality Security Assessor (“QSA”). According to the former Business Analyst, the QSA employees were “kind of sequestered in a corner” of the Heartland office and mostly kept to themselves. The QSA employees did not ask the former Business Analyst about whether her/his enhancements were PCI compliant or other details about her/his work.

90. Indeed, each of the Confidential Witnesses tell corroborating stories of the security issues at Heartland, Defendants’ knowledge of the December 2007

breach, and Defendants' failure to disclose the breach for more than a year. These material omissions by Defendants were intended to and did artificially inflate the price of Heartland's stock throughout the Class Period.

DEFENDANTS' CLASS PERIOD MATERIALLY FALSE AND MISLEADING STATEMENTS

91. The Class Period begins on February 13, 2008. On that date, Heartland announced its financial results for the fourth quarter and full year ended December 31, 2007. Later that evening, Defendants held an earnings conference call to discuss the Company's fourth quarter 2007 financial results. The Individual Defendants participated in the call on behalf of the Company. Though security and security spending was a hot topic on the call, Defendants made no mention of the major breach that had occurred at Heartland less than two months earlier:

Bob Carr – Heartland Payment Systems, Inc. President and CEO

* * *

As recently as 2004 margins were just a little north of 11%. In the fourth quarter the margin did fall but as Bob will explain in a minute the underlying margins in our business remain quite healthy. ***However, this quarter our operating margin was impacted by our decision to strengthen our disaster recovery and business continuity systems to support our growth plans.***

The new leadership in our IT group convinced me and our senior staff to make this investment now. We were also impacted by expenses in a few other areas including legal, marketing and rollout of our Express Funds product which ran ahead of expectations. Obviously I am disappointed about this and you can be sure that we will be deeply focused on managing these and all costs in the future.

* * *

Bob Baldwin – Heartland Payment Systems, Inc. CFO

* * *

Remember we accrued the buyout liability based on margin generated by existing merchants and with December's weakness this accrual came in low. G&A expenses rose 37% this quarter much higher than the more moderate growth we consistently achieved over the last few years. ***The increases were primarily driven by IT expenditures required to bolster our internal security and disaster recovery capabilities.*** In addition as Bob mentioned we had a host of what I call onetimers in everything from legal to marketing this quarter.

* * *

92. Later, in the question and answer session with analysts, Defendants were specifically asked about security spend from the past quarter:

Unidentified Participant

Bob, I wanted to ask you about the security spend you talked about or the IT spend. Was there a particular reason – I mean was there a necessity for this? Did you see the particular flaw that [made] you do this or was this just as a result of somebody else taking over and they felt there was a need for a spend?

Bob Carr – Heartland Payment Systems, Inc. President and CEO

Good question (inaudible) thank you. ***We were surprised frankly with some of the inadequacies in our disaster recovery in our business continuity model. We have moved to a data warehousing approach and just in the process of doing our planning for '08 we discovered a couple of things we felt made us more vulnerable than we wanted to be and we decided to take – go ahead and bite the bullet and do what we thought was the right thing and spend the money in the fourth quarter.***

So that we felt we could in good conscience say that we have a very very secure system and as much to the extent that we know how to

make it secure. So it was a surprise, it was a negative surprise that came as a result of us getting new information about some of what we had developed in the past.

* * *

93. Further, when asked directly, Defendants outright denied that a security breach had even occurred at Heartland:

Tony Wible – Citigroup Analyst

I was hoping we could go back into the disaster recovery investment. Can you just I guess tell us a little bit more about what prompted the review of the disaster recovery? *Was there a specific incident or was it a proactive review that triggered that thinking?*

Bob Carr – Heartland Payment Systems, Inc. President and CEO

There were a couple of things that we learned as we reassigned responsibilities. *We learned that there was – there were some significant vulnerabilities that thank goodness we didn't suffer any results from those vulnerabilities but we could have.* And I think this is true of a lot of IT shops frankly sometimes it's good to have new blood come in and take a look at the firewalls that are developed and the internal controls of the existing people.

And we just found that the veteran team had gotten comfortable with the systems they set up years ago and they weren't effective anymore. And so it's a combination of a number of things. We also decided to kill a contract for a datacenter that we were going to set up in the Southeast and we're keeping all that in Texas. And that's caused us to have to do a write-off of a space that we never occupied and we think for the long-term we made the right decision there as well.

Tony Wible – Citigroup Analyst

Just to be clear there was never any action? It was just a fresh look at it through some new personnel and you were able to identify an area that should have been highlighted?

Bob Carr – Heartland Payment Systems, Inc. President and CEO

I wouldn't say it's new personnel. It's new facts that became evident to senior management about some of the weaknesses in the firewalls and in the internal controls of our people.

Tony Wible – Citigroup Analyst

Was there any particular incident that triggered that? That's what I'm trying to get at is this something (multiple speakers).

Bob Carr – Heartland Payment Systems, Inc. President and CEO

The incident was that new people came in and looked at our systems and found a number of things which were just not acceptable.

Bob Baldwin – Heartland Payment Systems, Inc. CFO

We did have one what I call minor incident in terms of our spam aspect of our firewalls so we did have one two-day period when our e-mails were overwhelmed with offers to do all kinds of different things. But there was no other incident and that by the way sort of burned out our firewall and we had to do some emergency preventative things on that. But it was nothing in terms of a data security external intrusion. It was revaluation.

Bob Carr – Heartland Payment Systems, Inc. – President and CEO

We did learn that there was an unnecessary linkage between our payroll business and our card processing business that folks who were looking at payroll data were able to also look at card data and that was something that hadn't been planned on and we were surprised to learn and that caused us to invest some money to fix that right away as well.

* * *

Franco Turinelli – William Blair & Company Analyst

Thank you, that is helpful. And obviously we don't want to compare your guidance with consensus estimates because those were not endorsed by you. But certainly if you look at it relative to our expectations,

(inaudible) saying that you reported in the quarter and in terms of your guidance was at or above our expectations in terms of revenue, in terms of gross margin, in terms of merchant additions and all that stuff.

So everything seems to be going great except for this huge variance in the G&A cost and I guess I'm struggling with reconciling what I'm seeing as the fundamentals of the Company that you yourself had said were so good and seem to be being sustained if not even accelerating in some respects. I'm just really struggling with that decision to go ahead and spend several million dollars' worth at this time.

Bob Baldwin – Heartland Payment Systems, Inc. CFO

Let me give it a couple of comments. With IT security you're either pregnant or you're not. And I think it would be irresponsible for us to know that we have vulnerabilities in our system where we could have something really bad happen that would put the Company in a TJ Maxx position. Now fortunately we never had anything close to that happen but we could see a scenario where that could have happened. We don't see that anymore. Should we have spent that million plus dollars to fix the problem? I think we would have been irresponsible not to do that and we knew this wouldn't be a fun call as a result of that decision.

* * *

94. The statements in ¶¶91-93 were materially false and misleading when made and/or omitted material information because Defendants failed to disclose or indicate the following: (1) the Company was indeed “pregnant” because it had incurred a significant and material security breach in December 2007; (2) the Company had not fully resolved the issues arising out of the December 2007 security breach and did not ensure that the December 2007 security breach was contained; (3) due to Defendants’ failure to contain the December 2007 security breach, tens of

millions of consumers' credit card and debit card information remained compromised; and (4) that, as a result, the Company would face significant costs related to, among other things, liability and the implementation of proper measures to clean-up the breach, as well as significant damage to the Company's reputation and Defendants' credibility. Thus, Defendants' misrepresentations and omissions obfuscated the Company's true financial condition and future business prospects, artificially inflating the price of Heartland's common stock.

95. On or about March 10, 2008, Heartland filed its Annual Report with the SEC on Form 10-K, signed by each of the Individual Defendants, which stated, in relevant part:

* * *

Network Security

In the course of our operations, we compile and maintain a large database of information relating to our merchants and their transactions. We place significant emphasis on maintaining a high level of security in order to protect the information of our merchants and their customers. We maintain current updates of network and operating system security releases and virus definitions, and have engaged a third party to regularly test our systems for vulnerability to unauthorized access. Further, we encrypt the cardholder numbers that are stored in our databases using triple-DES protocols, which represent the highest commercially available standard for encryption.

Our internal network configuration provides multiple layers of security to isolate our databases from unauthorized access and implements detailed security rules to limit access to all critical systems. In response to potential security problems with payment processors' systems, Visa and MasterCard have implemented new audit procedures to highlight

and repair any security weaknesses in payment processors' systems. In November 2003, we were certified by Visa as having successfully completed their Cardholder Information Security Program (CISP) review of our payment processing and Internet-based reporting systems. In 2004, the Visa CISP requirements were combined with security guidelines of the other card networks into a comprehensive Payment Card Initiative Data Security Standard (PCI-DSS). We have maintained our compliance to this standard and received recent confirmation of compliance to the standard in February 2007.

Visa, Star, NYCE and other debit card networks have established security guidelines for PIN-based debit transaction processing that is based upon ANSI standards that are published as the "ASC X9 TG-3 PIN Security Compliance Guideline." We have regularly scheduled Security Review of our Key Management Procedures against this standard that is performed by an external auditor.

We also have engaged external auditors to perform an annual SAS-70 review and publish our "Report on Controls Placed in Operation and Tests of Operating Effectiveness." In addition, we have undertaken an independent Cyber-Risk Assessment.

* * *

Unauthorized disclosure of merchant and cardholder data, whether through breach of our computer systems or otherwise, could expose us to liability and protracted and costly litigation. We collect and store sensitive data about merchants, including names, addresses, social security numbers, driver's license numbers and checking account numbers. In addition, we maintain a database of cardholder data relating to specific transactions, including bank card numbers, in order to process the transactions and for fraud prevention. Any significant incidents of loss of cardholder data by us or our merchants could result in significant fines and sanctions by Visa, MasterCard or governmental bodies, which could have a material adverse effect upon our financial position and/or operations. In addition, a significant breach could result in our being prohibited from processing transactions for Visa and MasterCard.

Our computer systems could be penetrated by hackers and our encryption of data may not prevent unauthorized use. In this event, we

may be subject to liability, including claims for unauthorized purchases with misappropriated bank card information, impersonation or other similar fraud claims. We could also be subject to liability for claims relating to misuse of personal information, such as unauthorized marketing purposes.

These claims also could result in protracted and costly litigation. In addition, we could be subject to penalties or sanctions from the Visa and MasterCard networks.

Although we generally require that our agreements with our service providers who have access to merchant and customer data include confidentiality obligations that restrict these parties from using or disclosing any customer or merchant data except as necessary to perform their services under the applicable agreements, we cannot assure you that these contractual measures will prevent the unauthorized use or disclosure of data. In addition, our agreements with financial institutions require us to take certain protective measures to ensure the confidentiality of merchant and consumer data. Any failure to adequately enforce these protective measures could result in protracted and costly litigation.

* * *

Contingencies – The Company collects and stores sensitive data about its merchant customers and bank cardholders. ***If the Company's network security is breached or sensitive merchant or cardholder data is misappropriated, the Company could be exposed to assessments, fines or litigation costs.***

* * *

96. The statements in ¶95 were materially false and misleading when made and/or omitted material information because Defendants failed to disclose or indicate the following: (1) the Company had already incurred a significant and material security breach in December 2007; (2) the Company had not fully resolved the issues arising out of the December 2007 security breach and did not ensure that the

December 2007 security breach was contained; (3) due to Defendants' failure to contain the December 2007 security breach, tens of millions of consumers' credit card and debit card information remained compromised; (4) as detailed by the Confidential Witnesses, the Company did not place "significant emphasis on maintaining a high level of security;" (5) the Company lacked adequate internal controls; and (6) that, as a result, the Company would face significant costs related to, among other things, liability and the implementation of proper measures to clean-up the breach, as well as significant damage to the Company's reputation and Defendants' credibility. Thus, Defendants' misrepresentations and omissions obfuscated the Company's true financial condition and future business prospects, artificially inflating the price of Heartland's common stock.

97. On March 17, 2008, Hannaford Brothers Co. ("Hannaford") announced a security breach which exposed 4.2 million credit and debit card numbers and led to 1,800 cases of fraud. Hannaford said credit and debit card numbers were stolen from its systems during the card authorization process and about 4.2 million unique account numbers were exposed. Hannaford said the data was taken between December 7, 2007 and March 10, 2008, and Hannaford reported that it was first made aware of "unusual credit card activity" on February 27, 2008.

98. The Hannaford breach affected all of its 165 stores in the Northeast, 106 Sweetbay stores in Florida and a smaller number of independent groceries that sell

Hannaford products. According to Hannaford CEO Ronald C. Hodge, the data “was illegally accessed from [Hannaford’s] computer systems during transmission of card authorization.”

99. The Hannaford breach was big news in the media. A March 28, 2008 *Security Wire Daily News* article titled, “Hannaford breach details indicate inside job” noted:

* * *

Experts said the breach should serve as a big lesson for retailers: It’s as important to limit the network access of employees and regularly monitor system activity as it is to purchase security technology to block attacks from the outside. Furthermore, it’s foolish for a company to consider itself bulletproof because they achieved PCI DSS compliance, as Hannaford’s claims it did.

* * *

That assessment comes amid the buzz over Hannaford’s letter to Massachusetts Attorney General Martha Coakley and the Office of Consumer Affairs and Business Regulation, in which the Maine-based retailer concluded it was the victim of a “new and sophisticated” technique where the attacker sneaked malware onto servers at all of its nearly 300 grocery stores. The malware apparently snatched card data from customers as they swiped their card through the checkout counter machine and transferred the data overseas.

* * *

100. Defendants were well aware of the Hannaford breach at the time it was disclosed, as well as the similarities in the Hannaford breach to the breach that had already occurred at Heartland in December 2007. For instance, on August 12, 2009,

in an interview given to *Computerworld.com*, Carr stated “[i]mmediately after the Hannaford Supermarkets breach, where we learned a sniffer had been used, that was a whole new paradigm. That’s when we started working on end-to-end encryption. Data-at-rest encryption was no longer enough. Data in transit can be captured.” Yet, Defendants continued to make false and misleading statements and/or omissions about the breach that occurred at Heartland in December 2007, and continued to fail to take the necessary steps to adequately contain the breach.

101. Thereafter, on conference calls on May 1, 2008, May 5, 2008, and August 5, 2008, and press releases and other public filings on May 1, 2008, May 9, 2008, June 16, 2008, August 5, 2008 and August 8, 2008, and despite their knowledge of the December 2007 security breach, Defendants failed to disclose anything about the existence of the breach, thus perpetrating the ongoing misrepresentations regarding the Company’s true financial condition and future business prospects, maintaining an incorrect market perception built on Defendants’ false and misleading statements, and causing and/or maintaining the artificial inflation in Heartland’s stock.

102. The statements in the conference call transcripts, press releases and public filings referenced in ¶101 were materially false and misleading when made and/or omitted material information because Defendants failed to disclose or indicate the following: (1) the Company had already incurred a significant and material security breach in December 2007; (2) the Company had not fully resolved the issues

arising out of the December 2007 security breach and did not ensure that the December 2007 security breach was contained; (3) due to Defendants' failure to contain the December 2007 security breach, tens of millions of consumers' credit card and debit card information remained compromised; (4) as detailed by the Confidential Witnesses, the Company did not place "significant emphasis on maintaining a high level of security;" (5) the Company lacked adequate internal controls; and (6) that, as a result, the Company would face significant costs related to, among other things, liability and the implementation of proper measures to clean-up the breach, as well as significant damage to the Company's reputation and Defendants' credibility. Thus, Defendants' misrepresentations and omissions obfuscated the Company's true financial condition and future business prospects, artificially inflating the price of Heartland's common stock.

103. In August, 2008, Carr established a trading plan pursuant to SEC Rule 10b5-1.⁶

⁶ In 2000, the SEC adopted Rule 10b5-1, 17 C.F.R. §240.10b5-1, which provides that a person will be deemed to have traded "on the basis of" material, nonpublic information if the person engaging in the transaction was "aware of" that information at the time of the trade. *See Selective Disclosure and Insider Trading*, 65 Fed. Reg. 51, 716, at 51, 727 (Aug. 24, 2000). Pursuant to SEC Rule 10b5-1(c), a 10b5-1 plan is a defense to insider trading liability only if it is entered into by an insider "before becoming aware" of inside information, and was established "in good faith and not as part of a plan or scheme to evade the prohibitions" against insider-trading.

104. On September 22, 2008, having no knowledge of the major security breach that had occurred at Heartland due to Defendants' failure to disclose it to the public, and buying into Defendants' false and misleading Class Period statements concerning the quality and safety of the Company's security systems, InformationWeek named Heartland to its InformationWeek 500, citing Heartland's technology that delivers "secure payments-processing to Heartland's clients."

105. Purportedly in late October 2008, ten months after Defendants became aware of the breach, Visa contacted Heartland to report suspicious transactions stemming from accounts linked to Heartland's systems. According to Visa, the accounts appeared to have been subjected to fraudulent activity shortly after legitimate transactions were made. Publicly, however, rather than disclose the 10-month old December 2007 breach and its connection to the October 2008 problems, Defendants continued their fraudulent scheme and remained silent.

106. On November 4, 2008, Heartland announced its financial results for the third quarter ended September 30, 2008. Later that afternoon, Defendants held an earnings conference call to discuss the Company's third quarter 2008 financial results. The Individual Defendants participated in the call on behalf of the Company. Defendants again discussed the Company's security systems, but again failed to disclose the existence of the December 2007 breach:

* * *

Bob Carr – Heartland Payment Systems, Inc. Chairman, CEO

We also recognize the need to move beyond the lowest common denominator of data security. Currently the PCI DSS standards. We believe it is imperative to move to a higher standard for processing secure transactions. One which we have the ability to implement without waiting for the payments infrastructure to change. We believe that standard to be – we believe that standard to be true end-to-end encryption and we are committed to launching this new standard in the fourth quarter '09 or early 2010 with several forward-looking clients and industry partners. We believe that the payment world is at risk relying on virus protection software to protect us from determined criminal organizations. The development of the new Discover and American Express products is also progressing. We expect to be boarding new American Express installs by January 1, with Discover to follow in the first half of next year.

* * *

Anurag Rana – KeyBanc Capital Markets Analyst

Good morning, guys. Congratulations on a good quarter. Bob, just wondering about large customers. You have talked a while ago about the salesforce going after large merchants. Just wanted to see if there's been any success in that area and how you perceive that opportunity at this point?

Bob Carr – Heartland Payment Systems, Inc. Chairman, CEO

We think that's a great opportunity. It's been very interesting talking to the large customers that we acquired with Network Services. We're a one-stop shop in the fact that we can do front end, back end, and now gift and loyalty. Big merchants like that, so that everything is integrated into one. I think we're going to be a significant player in the years coming ahead. There's not going to be anything coming down in the next few months that I know about. It's going to shock the world, but I think we're going to be able to add a lot of value to many large merchants, and we can do it in a way that is profitable because of our integrated platforms. I think you are going to see a lot of activity there. *I also mentioned security. Security is a major driver of the interests of the – not just the payment departments of large companies, but of the*

corporate risk officers who are very concerned about the risks of the brand in the event of a TJ Maxx or a Hannifer [Hannaford] type problem, and the current platforms out there are not really, in my view, and in the view of a lot of the large merchants I talk to, they're not really adequate to meet the – to counter the criminal organizations that are hacking through in various ways. I think there's a lot of play going forward. I think the world is going to change a lot over the next few years with large merchants.

* * *

107. The statements in ¶106 were materially false and misleading when made and/or omitted material information because Defendants failed to disclose or indicate the following: (1) the Company's safety and security measures designed to protect consumers' financial records and data from security breaches were inadequate and ineffective, and were not a "major driver" of Heartland's interests; (2) the Company was not PCI DSS compliant; (3) the Company had already incurred a significant and material security breach in December 2007; (4) as detailed by the Confidential Witnesses, the Company did not place "significant emphasis on maintaining a high level of security;" (5) the Company had not fully resolved the issues arising out of the December 2007 security breach and did not ensure that the December 2007 security breach was contained; (6) due to Defendants' failure to contain the December 2007 security breach, tens of millions of consumers' credit card and debit card information remained compromised; (7) the Company lacked adequate internal controls; and (8) that, as a result, the Company would face significant costs related to, among other things, liability and the implementation of proper measures to clean-up the breach, as

well as significant damage to the Company's reputation and Defendants' credibility. Thus, Defendants' misrepresentations and omissions obfuscated the Company's true financial condition and future business prospects, artificially inflating the price of Heartland's common stock.

THE TRUTH BEGINS TO EMERGE

108. On January 20, 2009 (Inauguration Day), Heartland issued a press release titled, "Heartland Payment Systems Uncovers Malicious Software In Its Processing System." The press release stated, in relevant part:

Payments processor Heartland Payment Systems has learned it was the victim of a security breach within its processing system in 2008. Heartland believes the intrusion is contained. "We found evidence of an intrusion last week and immediately notified federal law enforcement officials as well as the card brands," said Robert H.B. Baldwin, Jr., Heartland's president and chief financial officer. "We understand that this incident may be the result of a widespread global cyber fraud operation, and we are cooperating closely with the United States Secret Service and Department of Justice."

* * *

After being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, Heartland enlisted the help of several forensic auditors to conduct a thorough investigation into the matter. Last week, the investigation uncovered malicious software that compromised data that crossed Heartland's network.

Heartland immediately took a number of steps to further secure its systems. In addition, Heartland will implement a next generation program designed to flag network anomalies in real time and enable law enforcement to expeditiously apprehend cyber criminals.

* * *

109. Thereafter, Defendants held a conference call to discuss earnings for the fourth quarter 2008. Discussion of the security breach dominated the call:

Bob Carr – Heartland Payment Systems, Inc. Chairman & CEO

* * *

On January 20, of '09, we announced the discovery of malware in our payment systems environment, apparently resulting from a criminal breach. Potentially exposed through this breach of the payment environment were card numbers, expiration dates and other data from the cards' magnetic stripe. In a small percentage of cases, the card holder name also appears to have been exposed. However, the card holder information we processed does not include addresses or Social Security numbers. We also believe that no unencrypted pin data was captured and we believe the breach has been contained and did not extend beyond '08.

In late October, we were alerted by Visa of suspicious activity surrounding certain accounts that appeared to certain issuers to have been subjected to fraudulent activity shortly after they were used to make legitimate transactions that were processed by Heartland. Our IT team worked with the brand to try to match the suspicious transactions with our processing activities. And we engaged forensic auditors to evaluate different parts of our processing platform to investigate whether there was a potential problem. Ultimately, one of those firms provided our team with information that led us to discover malware output files on January 12 and on January 13, led us to the discovery of malicious software that apparently had created these files.

These malicious software programs were able to read and collect data in unencrypted form as it was in motion, which is when it was being sent to the switches that transmit data to the card brands during the transaction authorization process. The intruder potentially may have been able to exfiltrate from the network some of the data collected by means of the malware.

Keep in mind that Heartland passed its PCI certification last April and assessors are currently on-site for the 2009 certification, which we are targeting to complete by the end of April. In that regard, throughout the

potential period of the breach, Heartland did have antivirus software installed on its payment processing network.

The length of time that the malicious software was on the servers is not clear, though at this time, we believe it ceased being active during 2008. Further, it seems clear that the malware was not active at all times during this period, and it was probably not capturing information from 100% of transactions flowing through the system even when active or exporting all of the captured information to the criminals. For this reason, it is simply not possible at this time to determine accurately the number of card accounts that had information placed at risk of compromise during the breach, or to what extent any such information placed at risk was in fact compromised.

Immediately upon discovery of the breach, we took a number of forward-looking steps. First, on January 13, we contacted the Department of Justice and the Secret Service as well as the card brands to notify them of the breach. While many facts were still unclear, we nonetheless made our public announcement on January 20, 2009. Then, in the days following the announcement, we contacted more than 150,000 merchant locations to help them understand this data breach and what we're doing to prevent future incursions.

* * *

Bob Baldwin – Heartland Payment Systems, Inc. President & CFO

* * *

Let me provide some perspective on the impact of the breach in our fourth-quarter results and our current expectations regarding their prospective impact. FAS 5 establishes the standards of financial accounting and reporting for loss contingencies. It requires accrual by a charge to income and disclosure for an estimated loss from our loss contingency if two conditions are met.

One, information available prior to issuance of the financial statements indicates that it is probable that an asset has been impaired or a liability had been incurred at the date of the financial statements. And, two, the amount of the loss can be reasonably estimated. Accruals for general or

unspecified business risks, reserves for general contingencies, are not permitted.

To date, we have had several lawsuits filed against us and we expect that additional lawsuits will be filed. We are also the subject of several governmental investigations and inquiries, including an informal inquiry by the SEC and a related investigation by the Department of Justice, an inquiry by the OCC, and an inquiry by the FTC, and we may, in the future, be subject to other governmental inquiries and investigations. We intend to vigorously defend any claims asserted against us and we believe we have meritorious defenses to the claims asserted against us to date.

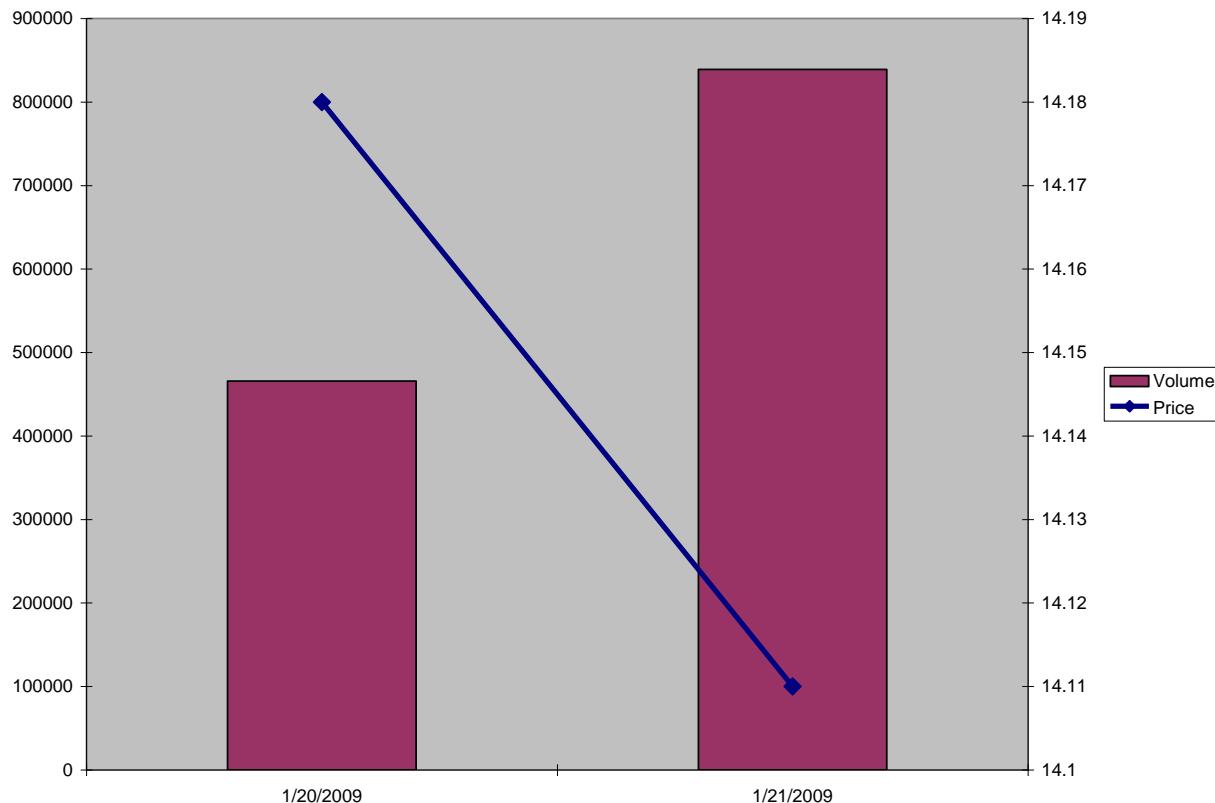
At this time, we do not have information that would enable us to reasonably estimate the amount of any losses we might incur by reason of such claims, and such losses are not currently deemed probable. We recognize, however, that we may incur losses in connection with the breach and that such losses could be material and could have a material adverse impact on our results of operations and financial condition.

In looking at comparable situations, we took several quarters after their breaches were discovered and announced before other companies could reasonably assess the magnitude of similar incidents, and therefore recognize a reserve for expected losses. The financial statements for the fourth quarter of 2008 include only immaterial [costs] we incurred related to investigations and remedial actions performed in December. We have not recorded a charge for estimated costs and expenses we might incur in connection with the breach since such costs and expenses are not yet reasonably estimable.

Clearly, as we look to 2009, we are very aware of the potential demands on our cash, primarily related to costs associated with the breach. We do not have the information to estimate any such potential costs, and it is likely to be some time before we have much clarity. However, these costs could be material. Currently, we expect that Heartland's cash generation capacity will be sufficient, combined with our strong balance sheet, to give us the capacity to absorb significant cost.

* * *

110. Upon release of this information, shares of Heartland declined \$1.26 per share, or 8.16%, to close on January 20, 2009 at \$14.18 per share, on unusually heavy volume, as set forth in the following chart:



111. On January 22, 2009, *Bloomberg* published an article titled, “Heartland Payment Breach May Trigger More Security Requirements.” The article noted that the breach may have involved 100 million accounts, which would have doubled the largest theft in history. The article, in relevant part, stated:

* * *

A computer break-in at Heartland Payment Systems Inc., the bank-card payment processor for 250,000 U.S. businesses, may prompt credit-card issuers to step up security before approving payments, analysts said.

“There have to be extra security precautions put into place,” said Curtis Arnold, chief executive officer of CardRatings.com, a Web site that reviews credit cards. The incident could involve 100 million accounts, Gartner Inc. analyst Avivah Litan said, citing sources in the banking industry. That would be twice the size of a 2007 attack on TJX Cos., owner of the T.J. Maxx and Marshalls discount chains, when hackers stole 45.7 million credit- and debit-card numbers, the largest such theft on record.

“Fundamentally, the bad guys are very, very good,” Heartland Chief Financial Officer Robert Baldwin said yesterday in an interview. “We’re deeply disappointed.” One potential security move may follow the lead of Citigroup Inc.’s Virtual Account Numbers program, which generates a unique number with limited uses for online purchases, Arnold said. Verified by Visa, which confirms the online shopper’s identity with an extra [question], is another “underutilized” program, he said.

“Malicious software that compromised data that crossed Heartland’s network” was found in the processing system last week, the Princeton, New Jersey-based company said in a statement Jan. 20. The breach occurred sometime in 2008, the company said.

Totally Speculative

Heartland doesn’t know how many accounts were affected and any estimate is “totally speculative,” Baldwin said.

Heartland fell 7 cents to \$14.11 yesterday in New York Stock Exchange composite trading. The shares lost 34 percent in the 12 months before today. Heartland set up a Web site to provide consumers with information about the investigation at <http://www.2008breach.com>.

The company discovered the breach after Visa Inc. and MasterCard Inc. warned of suspicious activity surrounding processed card transactions, Heartland said, without providing details. The attack apparently came through the Internet, not someone inside Heartland, Baldwin said.

“If you’re a criminal and attack that data from offshore, you reduce the risk of getting caught,” said Mark Bower, director of information protection solutions for Palo Alto, California-based Voltage Security

Inc., which provides encryption services. “It’s more lucrative than the traditional bank robbing.”

Consumer Liability

Heartland, which has insurance to cover a portion of the costs of the breach, doesn’t know how much of a charge the company will take because of the theft, Baldwin said. If a card is used fraudulently, a consumer is liable for a maximum of \$50.

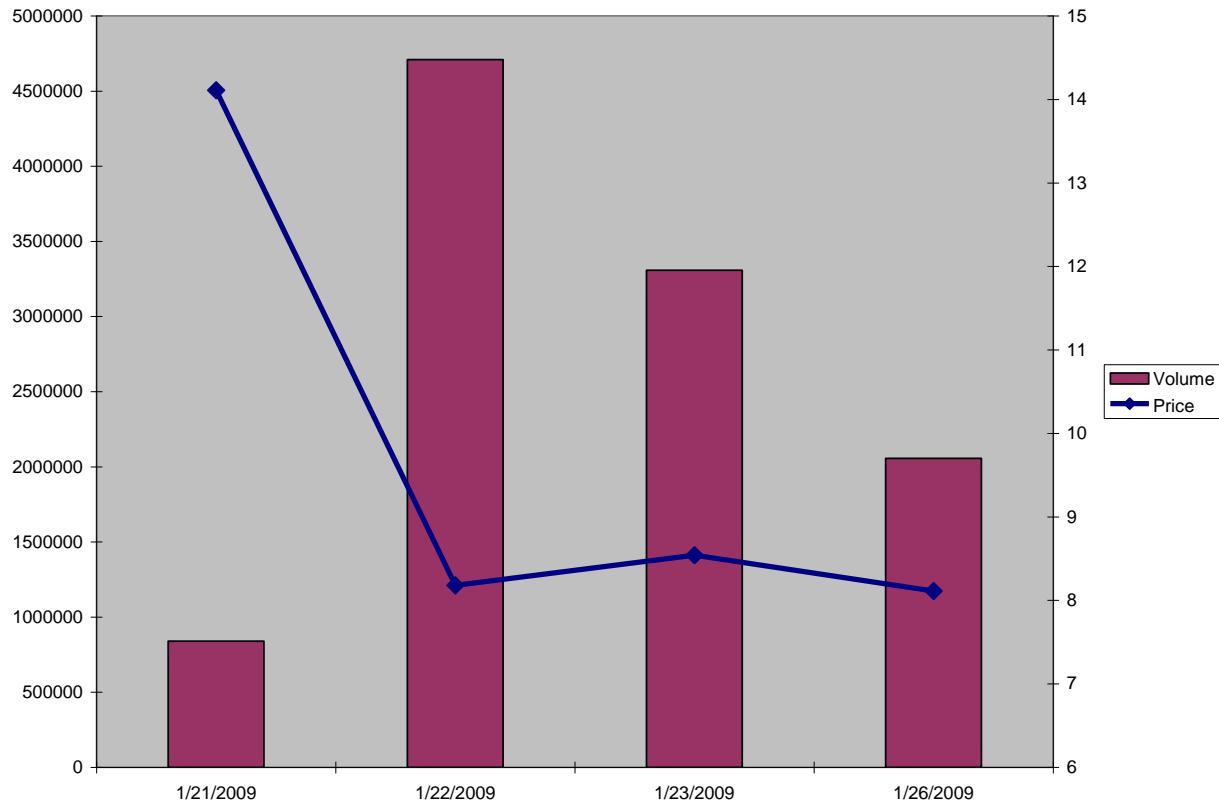
“This is obviously a huge liability for Heartland,” said David Robertson, publisher of the Nilson Report, which tracks the credit card industry. “The [question] is how many data breaches does it take for the industry to change?”

TJX agreed to pay as much as \$24 million to issuers of MasterCards and \$40.9 million to Visa issuers to cover fraud losses from its computer breach. Credit and debit card security should be more like that used by banks, said Eddie Woodruff, chief marketing officer at Lexington, Kentucky-based Forcht Bank, which reissued 8,500 debit cards because of the Heartland breach. To provide online security, banks ask [questions] that only the proper user could answer, such as the name of a school he or she attended.

“The online banking system has gone to multi-layer identification,” Woodruff said. “We will see that in debit cards as well.”

* * *

112. Based on this information, shares of Heartland declined an additional \$6.00 per share, or approximately 42%, to close on January 22, 2009 at \$8.18 per share, on extremely heavy volume, as set forth in the following chart:



113. Then, on February 24, 2009, Heartland issued a press release titled, “Heartland Payment Systems Reports Fourth Quarter Earnings of \$0.21 Per Diluted Share.” The press release stated, in relevant part:

* * *

Mr. Carr continued, “Heartland has been built on a foundation of fair dealings pricing transparency and merchant advocacy. Since our formation almost 12 years ago, our commitment to these principles has enabled us to grow into one of the largest companies in our industry. As the victim of a malicious system breach, we are highly focused on once again moving our industry forward, now taking the lead in strengthening the safety and security of information throughout the entire payments processing network. Heartland is committed to aggressively pursuing its efforts for the development and industry-wide implementation of end-to-end encryption technology – which if successfully developed and

implemented will be designed to protect data at rest as well as data in motion – as an improved and safer standard of payments security.

“Clearly our biggest challenge in 2009 will arise from the system breach we suffered. There are two main components to the challenge we face: addressing claims that cardholders, card issuers, the Brands, regulators, and others have asserted, or may assert, against us arising out of the breach and managing the potential impact of the breach on the day-to-day operations of our business.

With regard to the first challenge, we intend to vigorously defend any such claims and we believe we have meritorious defenses to those claims that have been asserted to date. At this time we do not have information that would enable us to reasonably estimate the amount of losses we might incur in connection with such claims. As to the second challenge, our sales and service teams have responded tremendously, and early indications of client response are positive: in the weeks since our announcement of the breach, we have installed more margin, and have a bit less merchant attrition, than in the same period in 2008.

While it is too early to tell, and we will certainly face challenges from macroeconomic conditions confronting our customers, at this point we believe that our expanded product breadth, reputation for superior customer service, candor, and no arbitrary rate increases, should allow us to grow our card processing merchants, payroll clients and check management clients in 2009. I am very proud of our Heartland employees, who are aggressively reaching out to strengthen our relationships and maintain the trust and confidence of the merchant community.”

* * *

FULL YEAR 2009 GUIDANCE:

Current economic conditions, the breach, and the financial climate are likely to influence same store sales growth and new merchant signings, necessarily adding conservatism to our guidance. For the year, we expect net revenue (total revenues less interchange, dues and assessments) to grow by 12 – 16%, to between \$430 and \$445 million, with 7 – 11% of that growth organic. For the year, earnings per share are expected to be \$1.15 – \$1.22. The Company’s guidance for 2009

does not include any estimates for potential losses, costs and expenses arising from the previously announced security breach, including exposure to credit and debit card companies and banks, exposure to various legal proceedings that are pending, or may arise, and related fees and expenses, and other potential liabilities, costs and expenses. Neither the costs nor the potential losses are estimable at this point, and further the potential losses are not currently deemed probable.

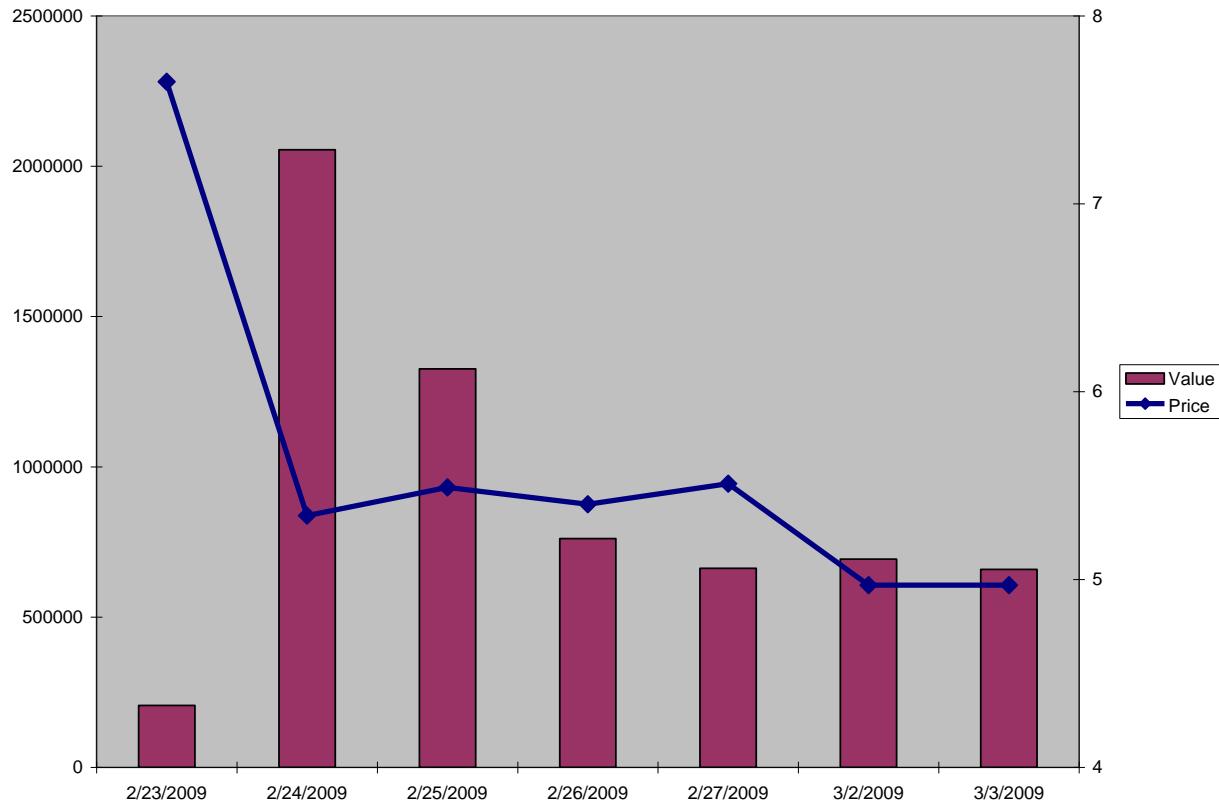
DIVIDEND:

The Company also announced that, in light of the difficulties in the financial markets, the Board of Directors believes it is prudent to maximize the Company's financial resources and liquidity. Consequently, ***the Board of Directors has established a new dividend rate and declared a quarterly dividend of \$0.025 per common share***, which is payable March 16, 2009 to shareholders of record on March 9, 2009.

* * *

114. Additionally, Heartland announced that it was under investigation by the SEC, United States Department of Justice, the United States Federal Trade Commission, and the Offices of the Comptroller of the Currency.

115. With this information, shares of Heartland further declined \$2.31 per share, or 30.12%, to close on February 24, 2009 at \$5.34 per share, on unusually heavy volume, as set forth in the following chart:



116. Following the February 24, 2009 conference call, KeyBanc Capital Markets released an analyst report noting:

We believe the stock's substantial decline today (down about 24% intra-day, compared with S&P 500 up roughly 2.5%) is a direct result of management's inability to provide investors with any more concrete details regarding its potential liability. We believe that the Company could not assure investors that it has sufficient resources to cover the potential cost of the breach. Partly along those lines, HPY's Board cut the Company's quarterly dividend by 75% to \$0.025/share.

ADDITIONAL SCIENTER ALLEGATIONS

117. In connection with the announcement that Heartland was subject to an SEC investigation, on February 29, 2009, Anthony M. Freed ("Freed"), Financial Editor for *Information-Security-Resources.com*, authored an article titled, "Heartland

Payment Systems Under SEC Inquiry – Another Red Flag”, wherein he set forth a timeline of events vis-à-vis Carr’s stock trades:

May 14, 2008: Breach reported to have began
May 20, 2008: Carr makes first stock sale of the year, consisting of 2,695 shares
August (first week), 2008: CEO Robert Carr’s 10b5-1 plan is proposed
August 8 – August 14, 2008: Carr makes six separate sales of stocks totaling 60,000 shares
August 19, 2008: Breach reported to have ended
August 28, 2008: Carr sells 80,000 shares
September 3, 2008: Carr sells 80,000 shares
September 17, 2008: Carr sells 80,000 shares
October 15, 2008: Carr sells 80,000 shares
October 28, 2008: Visa and Mastercard notify Heartland of problems; Carr sells 80,000 shares
November 6, 2008: Carr sells 80,000 shares
November 20, 2008: Carr sells 80,000 shares
December 11, 2008: Carr sells 80,000 shares
December 26, 2008: Carr sells 42,900 shares
January 7, 2009: Carr sells 80,000 shares
January 12, 2009: Carr suspends his 10b5-1 stock selling plan
January 20, 2009: Breach announced

118. Heartland quickly denied that Carr acted improperly in enacting his 10b5-1 plan. In response to the January 29, 2009 article by Freed, Heartland sent an email to Freed disavowing any wrongdoing:

At the time of this announcement, Mr. Carr was not under any trading restrictions pursuant to the company’s insider trading policy ***and was not in possession of any material non-public information concerning the company.*** Under this 10b5-1 plan, programmed sales of company stock were made on Mr. Carr’s behalf, and he had no discretion regarding the timing or other aspects of those sales.

Although he was not required to do so, Mr. Carr terminated his 10b5-1 when the company confirmed the security breach it disclosed in the

company's press release of January 20, 2009. As has been reported, Heartland first learned of a potential problem from the card associations on October 28th of last year, well after the announcement of this 10b5-1 plan. ***Heartland categorically denies that Mr. Carr was aware of a potential security breach at the time he adopted his trading plan.***

119. In response, Freed noted that as CEO of the sixth largest payment card processor, "I would hope that Carr would at times possess some non-public information on the company he built, but that is a topic for a different discussion on the overall CEO performance levels and our failing economy."

120. In any event, long after the January 20, 2009 disclosure of the massive security breach at Heartland, and in an apparent attempt to now cover-up their cover-up of the December 2007 breach, Defendants essentially admitted to ***Wired.com*** that **Defendants in fact knew all along that the security breach at Heartland had occurred in December 2007.** An August 17, 2009 *Wired.com* article titled, "TJX Hacker Charged With Heartland, Hannaford Breaches" noted in pertinent part:

* * *

Heartland's CEO Robert Carr told Wired.com recently that the initial breach into the company's network in December 2007 was confined to the company's corporate network, which Carr said was separate from its card-processing network. But by May 2008, the hackers had jumped to the processing network. Carr wouldn't say how they accomplished this (emphasis added).

* * *

121. Defendants' current position – ***in contrast to their Class Period statements wherein they essentially all but denied that a breach had occurred*** – is

that while they knew a security breach had occurred in December 2007 at the Company, they were under the impression that the breach was confined to the Company's corporate network, which was separate from its card-processing network. According to Defendants, Heartland caught the breach of the corporate network, but was unaware the hackers were sitting on its system for months conducting reconnaissance.

122. The timing of this complete reversal of position – indeed an admission of fraud – by Defendants is all the more suspicious given that it came the same week that the Department of Justice issued an indictment against the individuals who hacked into Heartland's systems indicating that the attack began on **December 26, 2007**.

According to the indictment issued on August 17, 2009:

[b]eginning on or about December 26, 2007, Heartland was the victim of an SQL Injection Attack on its corporate computer network that resulted in malware being placed on its payment proceedings system and the theft of more than approximately 130 million credit and debit card numbers and corresponding Card Data.

123. Then, on March 16, 2009, Visa announced that Heartland had been removed from Visa's list of PCI DSS compliant service providers. The press release stated, in pertinent part:

Removal from Visa's List of Compliant Service Providers – Visa has removed Heartland from its online list of Payment Card Industry Data Security Standard (PCI DSS) compliant service providers. HPS has advised, however, that it is aggressively working on remediation and re-validation of its systems to comply with PCI DSS standards. The company

will be relisted once it revalidates its PCI DSS compliance using a Qualified Security Assessor and meets other related compliance conditions.

System Participation – HPS is now in a probationary period, during which it is subject to a number of risk conditions including more stringent security assessments, monitoring and reporting. Subject to these conditions, Heartland will continue to serve as a processor in the Visa system.

124. The announcement by Visa that it had removed Heartland from its online list of PCI DSS compliant service providers was a further partial revelation of the insufficient level of data security at the Company, and corroborated the statements made by the Confidential Witnesses concerning the poor security, and inattention to PCI DSS compliance at Heartland.

APPLICABILITY OF THE PRESUMPTION OF RELIANCE: FRAUD ON THE MARKET DOCTRINE

125. At all relevant times, the market for Heartland common stock was an efficient market for the following reasons, among other things:

- (a) Heartland's common stock met the requirements for listing, and were listed and actively traded on the NYSE, a highly efficient and automated market; and
- (b) Heartland regularly communicated with public investors via established market communication mechanisms, including through regular disseminations of press releases on the national circuits of major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services.

126. As a result, the market for Heartland common stock promptly digested current information regarding Heartland from all publicly-available sources and

reflected such information in Heartland's common stock prices. Under these circumstances, all purchasers of Heartland common stock during the Class Period suffered similar injury through their purchase of Heartland's common stock at artificially inflated prices and a presumption of reliance applies.

LOSS CAUSATION

127. During the Class Period, as detailed herein, Defendants engaged in a scheme to deceive the market and a course of conduct that artificially inflated the value of Heartland common stock and operated as a fraud or deceit on Class Period purchasers of Heartland common stock by misrepresenting the Company's business success and future business prospects, including but not limited to misrepresentations regarding the Company's true exposure to non-prime/non-traditional mortgage loans, its capital adequacy, as well as its financial reporting.

128. As a result of Defendants' fraudulent conduct as alleged herein, the prices at which Heartland common stock traded were artificially inflated, at varying levels, throughout the Class Period. When Plaintiffs and other members of the Class purchased their Heartland common stock, the true value of such common stock was substantially lower than the prices actually paid by Plaintiffs and the other members of the Class.

129. During the Class Period, Defendants improperly concealed the truth regarding Heartland's financial performance and outlook, and future business

prospects. Consequently, the price of its common stock was artificially inflated throughout the Class Period. Defendants also misrepresented the reasons behind Heartland's reported results and made numerous false and misleading statements regarding many aspects of its business, including, but not limited to, failing to disclose the existence of the December 2007 security breach. Later, however, when the truth was revealed, Defendants' prior misrepresentations and fraudulent conduct became apparent to the market, the price of Heartland's common stock fell as the prior artificial inflation was removed from its share price. As a result of their purchases of Heartland common stock during the Class Period at artificially inflated prices, Plaintiffs and other members of the Class suffered economic loss, *i.e.*, damages under federal securities laws, when such artificial inflation dissipated.

130. By misrepresenting the success of the Company's business and concealing its improprieties, Defendants presented a misleading picture of Heartland's business and prospects. As a result of Defendants' materially false and misleading statements and documents, as well as the adverse, undisclosed information known to the Defendants, Plaintiffs and other members of the Class relied, to their detriment on such statements and documents, and/or the integrity of the market, in purchasing their Heartland common stock at artificially inflated prices during the Class Period. Had Plaintiffs and the other members of the Class known the truth, they would not have taken such actions.

131. As explained herein, these false statements directly or proximately caused, or were a substantial contributing cause, of the damages and economic loss suffered by Plaintiffs and other members of the Class, and maintained the artificial inflation in the prices of Heartland's common stock throughout the Class Period and until the truth leaked into and was partially revealed to the market, at which time the prior inflation came out of those common stock.

132. Defendants' false and misleading statements had the intended effect and directly and proximately caused, or were a substantial contributing cause, of Heartland's common stock trading at artificially inflated levels throughout the Class Period.

133. Through a series of partial disclosure events regarding the December 2007 security breach, which culminated in the acknowledgement by Defendants that Heartland might incur additional losses due to the security breach which, and the announcement that the Company was cutting its dividends by 72%, the market's expectations were ultimately corrected, and the artificial inflation came out of the prices of Heartland's common stock in fits and spurts. These events and disclosures caused one-time common stock drops of 8.16% on January 20, 2009, 42% on January 22, 2009 and 30.12% on February 24, 2009, and a total decline of almost 80% from Class Period highs.

134. The timing and magnitude of the declines in Heartland common stock negates any inference that the loss suffered by Plaintiffs and other Class members were caused by changed market conditions, macroeconomic or industry factors or Company-specific facts unrelated to the Defendants' fraudulent conduct. The economic loss, *i.e.*, damages, suffered by Plaintiffs and other members of the Class was a direct result of Defendants' fraudulent scheme to artificially inflate the price of Heartland common stock and their subsequent decline in value as Defendants' prior misrepresentations and other ongoing fraudulent conduct were revealed, market expectations were corrected, and the artificial inflation came out of Heartland's common stock.

135. In addition, the price of Heartland common stock was a natural and probable consequence of Defendants' fraud and should have been foreseen by Defendants in light of the attending circumstances. The market reactions to the partial disclosure of Heartland's true financial condition and future business prospects were foreseeable to Defendants and well within the "zone of risk" concealed by Defendants' fraudulent conduct.

NO SAFE HARBOR

136. The federal statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the allegedly false statements pleaded in this complaint. Many of the specific statements pleaded herein were not

identified as “forward-looking statements” when made. To the extent there were any forward-looking statements, there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements. Alternatively, to the extent that the statutory safe harbor does apply to any forward-looking statements pleaded herein, Defendants are liable for those false forward-looking statements because at the time each of those forward-looking statements was made, the particular speaker knew that the particular forward-looking statement was false, and/or the forward-looking statement was authorized and/or approved by an executive officer of Heartland who knew that those statements were false when made. Moreover, to the extent that Defendants issued any disclosures designed to “warn” or “caution” investors of certain “risks,” those disclosures were also false and misleading since they did not disclose that Defendants were actually engaging in the very actions about which they purportedly warned and/or had actual knowledge of material adverse facts undermining such disclosures.

COUNT I

For Violations of Section 10(b) of the Exchange Act and Rule 10b-5 Promulgated Thereunder Against All Defendants

137. Plaintiffs repeat and reallege the allegations set forth above as though fully set forth herein. This claim is asserted against all Defendants.

138. During the Class Period, Heartland and the Individual Defendants, and each of them, carried out a plan, scheme and course of conduct which was intended to and, throughout the Class Period, did: (i) deceive the investing public, Plaintiffs and other Class members, as alleged herein; (ii) artificially inflate and maintain the market price of Heartland common stock; and (iii) cause Plaintiffs and other members of the Class to purchase Heartland common stock at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Heartland and the Individual Defendants, and each of them, took actions set forth herein.

139. These Defendants: (i) employed devices, schemes, and artifices to defraud; (ii) made untrue statements of material fact and/or omitted to state material facts necessary to make the statements not misleading; and (iii) engaged in acts, practices, and a course of business which operated as a fraud and deceit upon the purchasers of the Company's common stock in an effort to maintain artificially high market prices for Heartland's common stock in violation of Section 10(b) of the Exchange Act and Rule 10b-5. These Defendants are sued as primary participants in the wrongful and illegal conduct charged herein. The Individual Defendants are also sued as controlling persons of Heartland, as alleged below.

140. In addition to the duties of full disclosure imposed on Defendants as a result of their making of affirmative statements and reports, or participating in the making of affirmative statements and reports, or participating in the making of

affirmative statements and reports to the investing public, they each had a duty to promptly disseminate truthful information that would be material to investors in compliance with the integrated disclosure provisions of the SEC as embodied in SEC Regulation S-X (17 C.F.R. §210.01, *et seq.*) and S-K (17 C.F.R. §229.10, *et seq.*) and other SEC regulations, including accurate and truthful information with respect to the Company's operations, surveillance, financial condition and operational performance, so that the market prices of Company common stock would be based on truthful, complete and accurate information.

141. Heartland and each of the Individual Defendants, individually and in concert, directly and indirectly, by the use, means or instrumentalities of interstate commerce and/or of the mails, engaged and participated in a continuous course of conduct to conceal adverse material information about the business, business practices, performance, operations and future prospects of Heartland as specified herein.

142. These Defendants each employed devices, schemes and artifices to defraud, while in possession of material adverse non-public information and engaged in acts, practices, and a course of conduct as alleged herein in an effort to assure investors of Heartland's value and performance, financial and operational growth, which included the making of, or the participation in the making of, untrue statements of material facts and omitting to state necessary facts in order to make the statements

made about Heartland and its business operations and future prospects in light of the circumstances under which they were made, not misleading, as set forth more particularly herein, and engaged in transactions, practices and a course of business which operated as a fraud and deceit upon the purchasers of Heartland common stock during the Class Period.

143. Each of the Individual Defendants' primary liability, and controlling person liability, arises from the following facts: a) each of the Individual Defendants was a high-level executive and/or director at the Company during the Class Period; b) each of the Individual Defendants, by virtue of his responsibilities and activities as a senior executive officer and/or director of the Company, was privy to and participated in the creation, development and reporting of the Company's financial performance, projections and/or reports; and c) each of the Individual Defendants was aware of the Company's dissemination of information to the investing public which each knew or disregarded with severe recklessness was materially false and misleading.

144. Each of these Defendants had actual knowledge of the misrepresentations and omissions of material facts set forth herein, or acted with severely reckless disregard for the truth in that each failed to ascertain and to disclose such facts, even though such facts were available to each of them. Even if Defendants were not shown to have actual knowledge of the misrepresentations and omissions of material fact set forth herein, Defendants' knowledge of this information can be inferred because the

misrepresentations and omissions of material fact set forth herein were critical to Heartland's core operations as a credit-card processor.

145. Such Defendants' material misrepresentations and/or omissions were done knowingly or with severe recklessness and for the purpose and effect of concealing Heartland's operating condition and future business prospects from the investing public and supporting the artificially inflated price of its common stock. As demonstrated by Defendants' misstatements of the Company's financial condition and performance throughout the Class Period, each of the Individual Defendants, if he or she did not have actual knowledge of the misrepresentations and omissions alleged, was severely reckless in failing to obtain such knowledge by deliberately refraining from taking those steps necessary to discover whether those statements were false and misleading.

146. As a result of the dissemination of the materially false and misleading information and failure to disclose material facts, as set forth above, the market prices of Heartland's common stock were artificially inflated, at varying levels, throughout the Class Period. In ignorance of the fact that market prices of Heartland common stock were artificially inflated, and relying directly or indirectly on the false and misleading statements made by Defendants, or upon the integrity of the market in which the common stock trade, and/or on the absence of material adverse information that was known to or disregarded with severe recklessness by Defendants but not

disclosed in public statements by Defendants during the Class Period, Plaintiffs and the other members of the Class acquired Heartland common stock during the Class Period at artificially high prices and were damaged thereby, as evidenced by, among others, the stock price declines identified herein that released the artificial inflation from Heartland's common stock.

147. At the time of said misrepresentations and omissions, Plaintiffs and other members of the Class were ignorant of their falsity, and believed them to be true. Had Plaintiffs and the other members of the Class and the marketplace known of the true performance, future prospects and intrinsic value of Heartland, which were not disclosed by Defendants, Plaintiffs and other members of the Class would not have purchased or otherwise acquired their Heartland common stock during the Class Period, they would not have done so at artificially inflated prices which they paid.

148. By virtue of the foregoing, Heartland and the Individual Defendants have each violated Section 10(b) of the Exchange Act, and Rule 10b-5 promulgated thereunder.

149. As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and the other members of the Class suffered damages in connection with their respective purchases and sales of the Company's common stock during the Class Period, as evidenced by, among others, the stock price declines identified herein that released the artificial inflation from Heartland's common stock.

COUNT II

For Violations of Section 20(a) of the Exchange Act Against the Individual Defendants

150. Plaintiffs repeat and reallege the allegations set forth above as though fully set forth herein. This claim is asserted against the Individual Defendants.

151. Each of the Individual Defendants acted as a controlling person of Heartland within the meaning of Section 20(a) of the Exchange Act as alleged herein. By virtue of their high-level positions with the Company, participation in and/or awareness of the Company's operations and/or intimate knowledge of the Company's fraudulent financial reporting and actual performance, each of the Individual Defendants had the power to influence and control and did influence and control, directly or indirectly, the decision-making of the Company, including the content and dissemination of the various statements which Plaintiffs contend are false and misleading. Each of the Individual Defendants was provided with or had unlimited access to copies of the Company's reports, press releases, public filings and other statements alleged by Plaintiffs to be misleading prior to and/or shortly after these statements were issued and had the ability to prevent the issuance of the statements or cause the statements to be corrected.

152. In addition, each of the Individual Defendants had direct involvement in the day-to-day operations of the Company and, therefore, is presumed to have had the

power to control or influence the particular transactions giving rise to the securities violations alleged herein, and exercised the same.

153. As set forth above, Heartland and the Individual Defendants each violated Section 10(b) and Rule 10b-5 by their acts and omissions as alleged in this Complaint. By virtue of their controlling positions, each of the Individual Defendants is liable pursuant to Section 20(a) of the Exchange Act. As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and other members of the Class suffered damages in connection with their purchases of the Company's common stock during the Class Period, as the artificial inflation dissipated from Heartland common stock.

WHEREFORE, Plaintiffs pray for relief and judgment, as follows:

A. Determining that this action is a proper class action and designating Plaintiffs as class representatives under Rule 23 of the Federal Rules of Civil Procedure;

B. Awarding compensatory damages in favor of Plaintiffs and the other Class members against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Awarding Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

D. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury.

DATED: August 20, 2009

COHN LIFLAND PEARLMAN
HERRMANN & KNOPF LLP
PETER S. PEARLMAN

s/Peter S. Pearlman

PETER S. PEARLMAN

Park 80 Plaza West-One
Saddle Brook, NJ 07663
Telephone: 201/845-9600
201/845-9423 (fax)

Liaison Counsel

COUGHLIN STOIA GELLER
RUDMAN & ROBBINS LLP
PAUL J. GELLER
DAVID J. GEORGE
JAMES L. DAVIDSON
BAILIE L. HEIKKINEN
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)

FARUQI & FARUQI, LLP
NADEEM FARUQI
EMILY C. KOMLOSSY
JAMIE R. MOGIL
369 Lexington Avenue, 10th Floor
New York, NY 10017-6531
Telephone: 212/983-9330
212/983-9331 (fax)

Co-Lead Counsel for Plaintiffs